(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平8－171535

(43)公開日　平成８年(1996)７月２日

(51)Int.Cl.⁶		識別記号	庁内整理番号	Ｆ Ｉ	技術表示箇所
Ｇ０６Ｆ	15/00	３３０　Ｚ	9364－5L		
	12/14	３２０　Ｂ			
		Ｃ			
Ｇ０９Ｃ	1/00		7259－5Ｊ		
				Ｈ０４Ｌ　9/00	Ａ

審査請求　未請求　請求項の数31　ＯＬ　（全 12 頁）　最終頁に続く

(21)出願番号　特願平6－239003

(22)出願日　平成６年(1994)10月３日

(31)優先権主張番号　０８／１３０１２６

(32)優先日　1993年10月４日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　594071860
アディソン・エム・フィッシャー
アメリカ合衆国　フロリダ州33942，ネイプルズ，マーチャンタイル・アベニュー，4073番

(72)発明者　アディソン・エム・フィッシャー
アメリカ合衆国　フロリダ州33942，ネイプルズ，マーチャンタイル・アベニュー，4073番

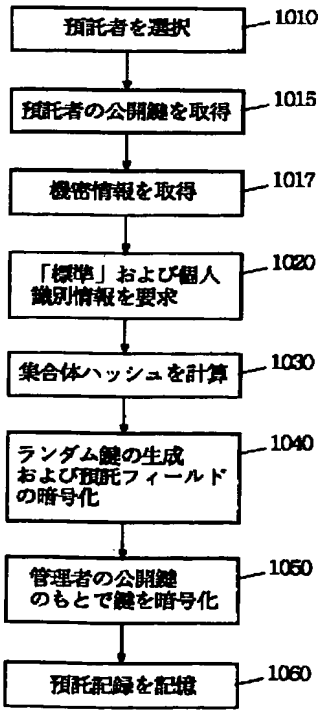
(74)代理人　弁理士　小笠原　史朗

(54)【発明の名称】　コンピュータ・データの機密保護方法

(57)【要約】　（修正有）

【目的】　預託された機密情報を持つ管理者が、情報受信の権利を有する関係者以外の人物に情報の漏洩を防ぐ方法と装置の提供。

【構成】　コンピュータ購入直後の任意の識別／定義局面と機密情報検索局面を用い、定義局面で、真実の所有者／顧客は、暗号化されたパスワードデータと自己識別データの預託記録を定義する。ユーザが、パスワード、または自分自身を独特に記述する一連の情報を入力す後に検索用の他の機密情報を自発的に預託する。識別印は、機密情報（ユーザの暗号化パスワードなど）と結合され、管理者の公開鍵の制御下で暗号化される。独特の識別データを入力後、ユーザは、システムを保護するためのパスワードを選択し、全ての個人識別データは、パスワードと共に、管理者の公開鍵を用いて暗号化され、例えば、ユーザのコンピュータ内に預託機密保護記録として記憶される。パスワードは、ユーザのディスク上の全データの暗号化に用いられる。



1

【特許請求の範囲】

【請求項１】　コンピュータユーザの機密デジタル情報が、後に管理者によって回復できるようにするためのコンピュータ操作方法であって、

特定のコンピュータユーザを識別するデジタル識別情報を確立するステップと、

識別情報にユーザの機密情報を結合させるステップと、

前記結合されたデジタル情報が管理者によってのみ解読可能なように、前記結合されたデジタル情報の少なくとも一部を暗号化するステップと、

暗号化されたデジタル情報を管理者による処理用に記憶するステップとを備える、コンピュータ操作方法。

【請求項２】　識別情報の少なくとも一部がハッシュ化される、請求項１に記載のコンピュータ操作方法。

【請求項３】　識別情報の少なくとも一部が平文で記憶される、請求項１に記載のコンピュータ操作方法。

【請求項４】　前記確立ステップは、コンピュータユーザに、複数のユーザ識別特徴データを提供させるステップを含む、請求項１に記載のコンピュータ操作方法。

【請求項５】　前記確立ステップは、ユーザが、身体的特徴情報を提供するステップを含む、請求項１に記載のコンピュータ操作方法。

【請求項６】　前記確立ステップは、ユーザが、ユーザの公開鍵を提供するステップを含む、請求項１に記載のコンピュータ操作方法。

【請求項７】　前記機密情報を回復する試みが為される場合に、管理者が従うべき命令をコンピュータユーザに要求するステップをさらに含む、請求項１に記載のコンピュータ操作方法。

【請求項８】　前記確立ステップは、前記機密情報を回復しようと試みる人物に対して、管理者が尋ねるべき少なくとも一つの質問を、ユーザが提供するステップを含む、請求項１に記載のコンピュータ操作方法。

【請求項９】　前記暗号化ステップは、

暗号化鍵を生成するステップと、

前記暗号化鍵を用いて少なくとも前記機密情報を暗号化するステップとを含む、請求項１に記載のコンピュータ操作方法。

【請求項１０】　前記暗号化ステップは、管理者の公開鍵を用いて前記暗号化鍵を暗号化するステップを含む、請求項９に記載のコンピュータ操作方法。

【請求項１１】　前記記憶ステップは、コンピュータユーザのメモリ媒体に前記暗号化されたデジタル情報を記憶するステップを含む、請求項１に記載のコンピュータ操作方法。

【請求項１２】　前記記憶ステップは、管理者を記述する情報を平文で記憶するステップを含む、請求項１に記載のコンピュータ操作方法。

【請求項１３】　管理者が、預託記録内に含まれる預託されたデジタル機密情報を申込者に安全に与えることができるようにするためのコンピュータ操作方法であって、

2

申込者を識別する信用証明書を取得するステップと、

預託された記録を取得するステップと、

預託された記録を解読するステップと、

申込者の信用証明証を、預託された情報内の識別情報と比較するステップと、

信用証明書が預託された識別情報と一致する場合に、申込者に機密情報を与えるステップとを備える、コンピュータ操作方法。

【請求項１４】　識別情報は、管理者が入手することのできる情報の一部として暗号化される、請求項１３に記載のコンピュータ操作方法。

【請求項１５】　識別情報のハッシュは、管理者が入手することのできる情報の一部として暗号化される、請求項１３に記載のコンピュータ操作方法。

【請求項１６】　前記預託情報が、紙上にデジタルフォームで印刷される、請求項１３に記載のコンピュータ操作方法。

【請求項１７】　識別デジタル情報は、氏名、住所、電話番号、身長、体重、誕生日、容貌、人種、目の色、出生地、会社、役職、事業地、社員証、上司、識別番号、デジタル化された指紋、デジタル化された写真、デジタル化された声見本、デジタル化された網膜情報、ユーザのＤＮＡに関する情報、デジタル化された筆跡見本、デジタル化されたキータイピング、筆法分析、ＤＮＡパターン、および一般的にコンピュータユーザ以外には知られていそうにない事実の内の少なくとも一つを含む、請求項１３に記載のコンピュータ操作方法。

【請求項１８】　解読ステップは、前記預託記録の少なくとも一部を解読するために管理者の個人鍵を使用するステップを含む、請求項１３に記載のコンピュータ操作方法。

【請求項１９】　解読ステップは、預託記録を解読するために管理者の個人鍵を使用し、預託記録内の他のフィールドを暗号化するのに用いられるランダム暗号化鍵をアクセスするステップを含む、請求項１３に記載のコンピュータ操作方法。

【請求項２０】　預託記録内の複数のフィールドのハッシュを計算するステップをさらに含む、請求項１３に記載のコンピュータ操作方法。

【請求項２１】　信用証明書が預託データに充分に一致しない場合は、申込者に更なる信用証明書を要求するステップをさらに含む、請求項１３に記載のコンピュータ操作方法。

【請求項２２】　前記要求ステップは、申込者に対して預託記録内で規定されている通りに質問をするステップを含む、請求項２１に記載のコンピュータ操作方法。

【請求項２３】　複数の管理者から機密情報の異なる部分を取得するステップをさらに含む、請求項１３に記載

のコンピュータ操作方法。

【請求項２４】　識別デジタル情報の少なくとも一部は、前記情報のハッシュによって示される、請求項１３に記載のコンピュータ操作方法。

【請求項２５】　処理装置、および当該処理装置に結合されるメモリ装置を有するコンピュータシステムにおいて、後に管理者がコンピュータユーザの機密デジタル情報を回復できるようにするために前記メモリ装置に記憶されるデジタルデータ構造であって、

コンピュータユーザを識別する識別情報を記憶する手段と、

暗号化された形で機密デジタル情報を記憶する手段とを備える、デジタルデータ構造。

【請求項２６】　前記管理者を識別する情報を記憶する手段をさらに含む、請求項２５に記載のデジタルデータ構造。

【請求項２７】　前記機密デジタル情報を暗号化するために用いられる暗号化鍵の暗号化されたバージョンを記憶する手段をさらに含む、請求項２５に記載のデジタルデータ構造。

【請求項２８】　前記識別情報および前記機密デジタル情報のハッシュを記憶する手段をさらに含む、請求項２５に記載のデジタルデータ構造。

【請求項２９】　前記識別情報記憶手段は、氏名、住所、電話番号、身長、体重、誕生日、容貌、人種、目の色、出生地、会社、役職、事業地、社員証、上司、識別番号、デジタル化された指紋、デジタル化された写真、デジタル化された声見本、デジタル化された網膜情報、ユーザのＤＮＡに関する情報、デジタル化された筆跡見本、デジタル化されたキータイピング、筆法分析、ＤＮＡパターン、および一般的にコンピュータユーザ以外には知られていそうにない事実の内の少なくとも一つを記憶する手段を含む、請求項２５に記載のデジタルデータ構造。

【請求項３０】　申込者が前記機密情報へのアクセスを得ようとする際に、管理者が従うべき命令を記憶する手段をさらに含む、請求項２５に記載のデジタルデータ構造。

【請求項３１】　管理者が、前記機密情報を回復しようと試みる人物に対して問うべき少なくとも一つの質問を記憶する手段をさらに含む、請求項２５に記載のデジタルデータ構造。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、一般にコンピュータ・データの機密保護に関し、より特定的には、預託された機密情報を持つ管理者が、その情報を受信する権利を正当に有する関係者以外の人物に情報を漏洩することを防ぐ方法および装置に関する。

【０００２】

【従来の技術】現代のコンピュータシステム、特にパーソナル・コンピュータまたはラップトップ・コンピュータを使用しているシステムにおいては、例えばディスクメモリなどに記憶されたデータを暗号化するのが一般的である。そのことにより、記憶されたデータは、コンピュータが盗まれた時でさえ泥棒によって発見されず、ユーザに厚い保護を提供する。

【０００３】一般に、そのような記憶された情報は、ユーザのみが知っているパスワードからある方法で導き出された鍵によって暗号化されている。パスワードは、周知の暗号処理技術により暗号鍵に変換され、その暗号鍵は、コンピュータに記憶されているあらゆる情報を解読する（その後、すべての情報にアクセスする）ために使用される。

【０００４】最も標準的な慣用機密保護方法では、機密データが記憶されている場合は特に、パスワードが相手によって発見されないようにするために、ユーザにパスワードを記録しないようにさせる。コンピュータに記憶されているデータは、暗号化された形でのみ存在しているので、パスワードを知らなければ、どのような実用目的のためにも、そのデータにアクセスすることはできない。従って、ユーザがパスワードを忘れた時に深刻な問題が生じるのである。

【０００５】実際に、ユーザは、時々自分のパスワードを忘れることがある。また、機嫌を損ねている従業員が、自分に割り当てられている会社のコンピュータ用のパスワードを供給することを拒んだり、またはパスワードを忘れたりする可能性もある。

【０００６】この問題に対する一つの解決法としては、パスワード（またはその暗号化に関連する他の鍵情報）を、管理者、すなわち信用のおける人物、例えば、ユーザの組織内のコンピュータ機密保護ソフトウェア保管者などに預託することである。ユーザは、機密情報を暗号化したり、その情報を記憶させるために、例えば管理者、第三者、または保護されているコンピュータ自身と、管理者が持っている公開鍵を共用してもよい。この方法により、管理者は、緊急の場合に預託された暗号テキストの結果を取り出すことができ、また自分の個人鍵を用いて預託された機密を解読したり検索することもできる。

【０００７】ユーザが受託者に良く知られている場合、機密情報を取り出す手順はかなり簡単である。管理者に良く知られているユーザが、預託すべき情報（できればコンピュータ全体を含む）を管理者に提供し、管理者は、ユーザの機密情報を解読するために自分の個人鍵（公開／個人鍵の対の片一方であり、管理者の暗号化公開鍵と関連する）を用いて預託された情報を取り出す。ユーザに対しては、管理者に預託する情報を検索するためのプログラムが供給されてもよい。管理者が解読用の個人鍵にアクセスしさえすれば、預託された情報がユー

ザのコンピュータ内の預託情報の記憶機構に妨害されることはない。

【０００８】

【発明が解決しようとする課題】本発明は、管理者が、騙されて正当な所有者（またはその預託情報を受け取る権利のある他の関係者）以外の人物に、預託された情報を漏洩する危険性を指摘している。例えば、泥棒が、盗んだコンピュータを自分のものであると管理者に対して主張することもあり得る。

【０００９】実際、パスワードを忘れたり、または紛失したと言うユーザが、コンピュータデータ暗号化製品のベンダに助けを求めることも珍しいことではない。ユーザは、どんなに忠告を受けていても、ベンダが自分の記憶情報を回復してくれると期待している。例えば、重要な情報が泥棒に漏れた場合の責任を恐れるなどの理由から、ベンダがユーザの手助けをできない、またはしないとしたら、本当のユーザは大概怒り出すであろう。ベンダにとって危険なのは、その仮のユーザが実際にその機密データの真の所有者でないかもしれないが、それどころか真の所有者のライバル（例えば、コンピュータにアクセスさせた人物が、真の所有者に対して大きな損害を与える可能性のある人）であるかもしれないことである。ゆえに、ベンダは、大抵は取り乱している顧客のために失われた鍵を「使用再可能」にするのを手伝うかどうかのジレンマに直面するであろう。

【００１０】本発明に従えば、様々な二者択一のバイナリデータストリングを預託することができる。ユーザの機密を暗号化するために用いられる対称ＤＥＳ暗号鍵を引き出すために使用されるパスワードは、預託することが可能である。広義では、本発明は、管理者の手中にある任意の機密デジタル情報（例えば、スイス銀行の口座番号、貸金庫の身分証明印、金庫室番号の組み合わせ、コカ・コーラ^{R} の製法など）をも預託することを考慮している。本発明は、ユーザがそのようなデータを暗号化して保護することができるようにし、また、ユーザがパスワードを忘れたり、紛失した場合に、メーカー、ベンダ、または他の受託者（管理者）が、ユーザをデーターにアクセスさせることができるようにする。

【００１１】本発明は、たとえ預託を受けた者（例えばベンダ）が事前に真の所有者または顧客を知らない場合でさえ、ベンダが、機密保護を供給するという本来の目的と、鍵を回復させるという副次的目的とを比較考慮しながら、不注意に機密を漏洩してしまう危険性をすっかり取り除くのではないとしても、減少するように設計されている。本発明は、管理者が、失われた鍵またはパスワードの使用を再び可能にするのを手伝う際に、寄せられた信頼を裏切ることがないことをユーザおよび管理者本人に対して保証する。

【００１２】

【課題を解決するための手段】本発明は、例えば、コンピュータを購入した直後などに実行される自発的識別／定義局面と、機密情報検索局面とを用いた手法を利用することによって、これらの目的を達成する。定義局面では、真の所有者または顧客が、暗号化されたパスワードまたは他の機密データと共に、自己識別データを供給する預託記録を定義する。本発明は、ユーザが自分自身を独特に記述した一連の情報を後の検索用に入力することにより、パスワードまたは他の機密情報をユーザが自発的に預託するよう促すことを考慮している。その識別印は、機密情報（例えばユーザの暗号化パスワードなど）と結合され、その後、管理者の公開鍵の管理下で暗号化される。これを行う方法は多数あり、本明細書で挙げた例は一例であって、包括的なものではない。例えば、結合された情報を任意の対称鍵（ＤＥＳ暗号など）のもとで暗号化してもよい。その場合、その後対称鍵は、管理者の公開鍵のもとで暗号化される。

【００１３】本発明の実施例においては、ユーザは、特有の識別データを入力した後に、システムを保護するためにパスワードを選択するよう求められる。その後、全ての個人識別データが、そのパスワードと共にメーカー（管理者）の公開鍵によって暗号化され、例えば預託機密保護記録としてユーザのコンピュータ内に記憶される。パスワードは、その後ユーザのディスク内のあらゆるデータを暗号化するために用いられる。

【００１４】将来ユーザがパスワードを忘れた場合、本出願人発明の検索局面が実行される。そのような状況下では、ユーザは、管理者、例えばベンダまたはメーカーに連絡を取る。本発明の実施例の一つとして、ユーザ（申込者）は自分の身元を明確に証明する証書を準備しなければならない場合もある。その証書は、公証人の前で作成された宣誓供述書の形を取ってもよいし、または十分に証明された公開鍵（または預託情報自身に示されている公開鍵）によって証明できるデジタル署名付メッセージを用いてもよい。身元を確認するために、運転免許証の提示、管理者による独自の調査、または申込者の立ち会いが必要なこともある。本発明の実施例の一つとして、ユーザは、例えば公証人の前で作成された身分証明書、申込者の立ち会い、または有効な運転免許の提示などを要求することによって、鍵（または他の機密情報）を時々検索しなければならない場合に、どのような機密保護手段が必要であるかを、最初に預託記録を設定する際にベンダに対して明確にするよう求められる。これにより、真の所有者が回復手順を要求するのを許容することができる。

【００１５】管理者は、預託された機密を検索するために、ユーザの証書および暗号化された預託情報を受け取らなければならない。これらのものが管理者に提示される順序はそれぞれのケースによって異なる。例えば、管理者（または他の第三者）が預託された情報を記憶するというモデルにおいては、ユーザが、その預託情報を

（その情報を作成した際などに）抽出して管理者に送信するのは簡単であろう。管理者が鍵回復サービスを供給するベンダである場合のモデルにおいては、ユーザは、（申込者の要求に応じて）ベンダが供給するユーティリティーの助けを借りなければ、預託された暗号テキストを抽出することができない方が好ましいかもしれない。そのユーティリティーは、（申込者の身元が、預託された個人識別と一致することを確認する前に）申込者の身元を確認した後のみに、申込者に供給される。極端なモデルにおいては、管理者は、鍵を抽出する前に装置に対して身体的にアクセスする（または所有物をアクセスさせる）ことさえ要求されることもある。この後者の要求によって、管理者は、装置を正当な所有者に、より簡単に返還することができるようになる。管理者は、預託記録を取得した後、その預託情報を解読し、申込者の証書と預託情報の真の所有者によって規定された身元確認法とを比較する。管理者は、仮のユーザが提示した証拠書類を用いて、その証拠が、ユーザによって作成されて先に暗号化されている預託記録内に記憶されている預託情報と一致するかどうかを決定する。それらが一致致すれば、管理者は、真の所有者が要求をしていると確信し、また個人鍵を与えることで所有者の利益を損なうことはなく、かつ可能な限りの合法的行動をしたことになると確信できる。

【００１６】申込者の証書が申込者の身元を確証している（ようである）が、要求されるレベルの確実性がない、つまり管理者が要求する証拠品としてのレベルに達していない、もしくは恐らく最初に設定された要求、または機密および識別が預託された時点で真の所有者によって要求された要求の内の一部しか満たしていない場合、その申込者の証書は疑わしいかもしれない。

【００１７】申込者の証書と預託情報が一致しない場合、管理者は、次のような適切と思われる行動を取ることができる。例えば、預託された情報に示される識別に基づいて真の所有者を見つけ、偽装が試みられたことを知らせる、明らかに盗まれたと思われるコンピュータを真の所有者に返す目的でそれを取り上げようと試みる、犯罪の容疑を警察またはその他の関係当局に知らせる、もしくはその申込者は真の所有者ではないが、（恐らく雇用者であるなどの理由から）正当にアクセスする権利を実際に有するかもしれないと判断するなどである。最後のケースであれば、申込者は管理者に最初にその旨を告げ、十分な追加の証書を提示したであろう。

【００１８】別の実施例においては、様々な識別事実の内で、（もしあるならば）暗号化された部分外にあって預託情報内に現れるものを決定し、暗号化された部分に識別事実がどれくらい現れるかを決定することができる。全ての識別情報を暗号化することが望ましいかもしれない。それにより、攻撃者が「なりすまし」をもくろむ手がかりが殆どなくなる。他に、（より無害な）情報の内の幾つかをクリアテキスト内の預託記録に記憶しておくと、紛失した場合に、その装置の正当な所有者を協力者に知らせることができる。

【００１９】本発明の典型的な実施例を示す添付図面を参照しながら、次の詳細な説明および特許請求の範囲の欄を読むことにより、本発明の上記および他の特徴および利点ならびにそれらを実現する方法がより明確になり、本発明がより理解し易くなるであろう。

【００２０】

【実施例】図１は、本発明を使用し得る典型的な通信システムを示すブロック図である。システムは、例えば電話回線または他の安全性が保証されていない通信路などの通信路１２を含み、その上で端末装置Ａ，Ｂ，…間の通信が行われる。図１に示すシステムの例においては、端末装置Ａは、受託者、管理者またはベンダによって使用されるデータ処理システムを表している。端末装置ＢからＮは、ユーザベースのコンピュータ端末装置を示し、その正当な所有者は、後述の方法に従って、ベンダを利用してパスワードまたは機密情報を預託する。

【００２１】端末装置Ａ，Ｂ，…Ｎはそれぞれ、例えばＩＢＭのＰＣ主記憶装置付互換処理装置２を含み、その処理装置は従来のキーボード／ＣＲＴディスプレイ４に結合されている。ベンダのデータ処理システム（端末装置Ａ）は、さらに公開／個人鍵の対の内の少なくとも個人鍵を記憶するための秘密個人鍵記憶装置５を含む。記憶装置５の内容は、演算処理装置２のみがアクセスできる。処理装置２は、個人鍵記憶装置５に記憶されている個人鍵を用いて預託暗号テキストを解読することにより、平文の預託情報を検索する。処理装置２は、トロイの木馬プログラムまたは他のウイルスによって悪影響を及ぼされる可能性を減少させる目的から、権利を有さない従業員または泥棒による不正使用に対して敏感な安全処理装置であってもよい。記憶装置５は、ベンダの従業員も判断できないほど安全に、記憶装置、すなわち個人鍵の内容を保管する（演算処理装置２用のプログラム・メモリとして使用することが可能な）読取専用記憶メモリ（ＲＯＭ）が好ましい。記憶装置５は、所望するならば演算処理装置２に含んでもよい。

【００２２】後に説明するように、ユーザのパスワードおよび／または他の機密情報を含む預託記録は、また、管理者の端末装置Ａに（作成直後またはパスワード検索処理の間に）記憶される。パスワードを安全に記憶するためのいかなる方法も有効である。

【００２３】端末装置Ａ，Ｂ，…Ｎは、また、従来のモデム６，８，１０にそれぞれ接続された際にメッセージの送信および受信ができる従来のＩＢＭ通信ボード（図示せず）を含む。各端末装置は、要求されるどのような暗号化操作およびデータ処理操作をも実行して、メッセージを作成することができる。ベンダの端末装置Ａは、ユーザから預託情報を受信するために通信路１２に結合

される形で示されているが、ユーザとベンダ間の通信は必ずしも電話連結を通じる必要はない。預託情報は、ベンダの端末装置の処理装置２に関連するフロッピーディスク読取装置に挿入されているフロッピーディスクを介して、ベンダの端末装置に送信することもできるし、または端末装置全体を管理者のもとへ運ぶことも可能である。

【００２４】端末装置Ａ，Ｂ…Ｎは、また、要求があればメッセージに暗号化操作を遂行することができる。本件に援用し、本出願の発明者の合衆国特許番号第４８６８８７７号および第５２１４７０２号に記載しているような周知の公開鍵暗号化方法を用いて、デジタル署名操作を遂行してもよい。

【００２５】図１は、ベンダの端末装置Ａのみを示しているが、本発明は機密分割鍵についても考慮しており、それによって、一人またはそれ以上の管理者が預託すべきユーザの機密の「分割鍵」の一部を受け取る。この場合、各管理者は、また、適切なユーザの（同一または異なる）ＩＤを受け取る。各管理者に異なる個人のＩＤ情報を分配することにより、一人の裏切り者の管理者が、他の管理者を騙してそれぞれの機密を暴露させて、必要な情報を全て知るという可能性を削減する。

【００２６】預託された情報は、他の情報から独立して維持および／または抽出することができる。例えば、機密情報がユーザのハードディスク上のデータを暗号化するために用いられるパスワードである場合、ユーザは、通信路１２を介して管理者に孤立した預託情報を届けるだけで、そのハードディスクを所有し続けることができる。この場合には、預託情報が、パスワード情報を回復する目的で設計されるのと同一のパスワード情報のもとで、その預託情報をまた暗号化することのないように注意する必要がある。預託記録が預託された暗号鍵と同一の暗号化されたハードディスクに書き込まれる場合、預託記録は、この暗号化によって保護されていない領域に書き込まれなければならない。このことは、預託された情報が管理者の公開鍵のもとで暗号化されているため、容認し得る。この場合、ハードディスクから預託記録を抽出するための特別のプログラムを使用することができる。この孤立した情報は、その後管理者に伝達される。

【００２７】危機が生じた場合の便宜のために、管理者の氏名、住所、電話番号などを預託情報と共に平文で保管しておくこともできる。それにより、ユーザは、この情報を古いファイルから探し出す必要が無くなる。預託された情報の２進数表示を紙に印刷し、管理者が緊急の場合にアクセスできるように、それを持っておくことも場合によっては望ましいかもしれない。管理者がそれを処理する前に、そのような印刷されたデータをコンピュータに再入力する必要があるだろう。これらの各実施例においては、管理者は、預託された鍵のもとで暗号化されている実際のデータにアクセスする必要は全くない。

【００２８】本発明の典型的な実施態様に従う動作において、ユーザは、例えば、図１に示す端末装置Ｂなどのコンピュータシステムを購入した直後、システムのセットアップ操作の間に、自分の身分を証明するための個人識別データを含む預託記録を生成するよう促される。そのような識別情報には、図２に関連して後述する識別証拠品を含めてもよいし、また、例えば図３において質問され、返答される質問を含めてもよい。その質問は、ベンダが、紛失または忘れられたパスワードの正当な所有者であると主張する人物を、追跡することを可能にする一連の質問であってもよい。正当な所有者または所有権を有する者（例えば権限を付与されている会社の雇用者）は、機密情報が失われた場合に、管理者が使用すべき好ましいプロトコル、および不正行為を疑われている場合にすべきことを要求する「機密メッセージ」を提供する。この情報は、その後、ベンダの公開鍵と共に暗号化される預託情報記録内に書き込まれる。

【００２９】パスワード情報または機密情報が失われ、ベンダがそれを検索する必要が生じた場合、ユーザは、端末装置Ｂにおいて、モデム６および８を介してベンダまたは管理者に預託記録を伝送する。その後、ベンダは、機密記憶装置５に記憶されている個人鍵を用いて預託情報を解読し、続いて預託情報を（後述するように）照合し、例えば本来の端末装置Ｂの所有者が規定した質問をすることによって、ユーザの身元を認証する。身元が認証されれば、パスワードは安全な方法で通信路１２を介して（適切に身分証明された）依頼者に伝達される。他に、機密個人鍵を記憶し、安全に保持する実施態様、および預託情報を処理する実施態様もまた、考慮している。例えば、機密鍵情報またはパスワード情報をスマートカードに記憶しておくことができ、そのカードには、要求された機密情報を検索するための操作をトリガするために個人識別番号を入力しなければならない。

【００３０】図２は、コンピュータの正当な所有者または所有権を有する者を識別するために収集される「標準」預託情報（１８）を示しており、（例えば氏名、住所などの）データ特徴を規定したデータ・フィールドを含む。標準預託情報デジタル図表は、さらに、記憶されたデータのタイプを識別する「トークン」（例えば、テキスト、バイナリ、ハッシュなど）および識別された特徴（例えば特定の氏名、住所など）と一致する特定の情報を識別する値フィールドを含む。

【００３１】図２に示す典型的な「標準」預託情報は、図４の８４に関連して後述する預託記録の一部として組み込まれる。識別情報は、好ましくは、管理者が選ばれ、限定された際にユーザによって供給され、例えば、ユーザの氏名２０、住所２２、誕生日２４、出生地２６、電話番号２８、ユーザの公開鍵３０、会社名３２、役職３４、上司の氏名３６、社員番号３８、社会保険番号４０、および運転免許証番号４２などの情報を含む。

図２に示すように、識別データは、ユーザの身長４４、体重４６、人種４７および目の色４８などの身体的な情報にまで及んでもよい。身体的情報は、デジタル化された写真５０、指紋５２、網膜パラメータ５４、声紋メッセージ５６、筆跡イメージ５８、筆法情報６０、さらにはデジタル化されたＤＮＡパターンなどの複合デジタル化情報を含んでもよい。また、所望するならば、多くの二者択一の識別特徴または追加の識別特徴（６４）を指定してもよい。所望するならば、そのような身体的特徴の情報のいくつかを、公証人などの公平な判定者によって書類で立証し、申込者の要求の一部として管理者に供給してもよい。標準識別情報は、さらにユーザのみが知っている個人的な事実、例えば好きな食べ物、古くからの友人の名前などを含んでもよい。管理者は、より説得力のある身分証明を引き出す手段としてこの情報を用いることができる。

【００３２】当該識別情報の内の幾つかは量的に大きくなりがちであり、他のデータベース内で非直結のまま保持されることが可能なため、デジタル化されたデータの（例えばＭＤ５またはＳＨＡを用いる）ハッシュのみを、預託記録内に含む必要がある。例えば、ユーザが、識別トークン、もしくは組織のＸ．５００辞書の中に記憶されている標準または公式のデジタル化された写真を持っている場合、ユーザは、預託記録内にこのイメージのハッシュを含めるだけでよい。ユーザは、管理者に検索依頼をする際に、管理者が公式のデジタル化された写真のコピーを確実に持っているようにする必要がある。この追加の情報のハッシュは、預託記録の内で特定されているハッシュと一致しなければならない。その後、預託記録に関連する定義情報は全て、ユーザ自身（声、身長、容貌、年齢など）、またはユーザの認証書類（運転免許証、社員証、公証人の宣誓供述書など）と比較される。

【００３３】現在の好ましい実施例によると、預託すべき機密情報を伴う識別データ（およびそのハッシュを伴う該集合体）は、管理者の公開鍵のもとで暗号化され、記録されるランダムＤＥＳ鍵のもとで暗号化される。管理者は、最終的な検索要求の一部として、預託記録内のハッシュによってのみ参照される情報のソースを提示されなければならない。また、幾つかの実施態様においては、幾つかの識別データ（例えば、氏名以外の全データ）を暗号化することのみが考慮される。（管理者以外には）隠されている定義識別の内の幾つかまたは全てを保持することで、攻撃を決意した人物が、模倣または偽造すべきものを知る機会を減少できる。

【００３４】定義情報は、ユーザによって明瞭に提供される必要はなく、ユーザの代理人、例えばユーザの上司、または実際のユーザに代わって基礎となる機密保護システムをインストールする企業の機密管理者が、機密を預託または供給する際に入手できる他の情報によって自動的に決定されてもよい。

【００３５】図３は、他の命令または情報、もしくは管理者に対するアドバイスを伴う（ユーザに対して後に質問される個人的知識を示す）典型的な「個人」識別情報データを示す。例えば、図３に示すように、ユーザは、パスワード情報を探している仮の所有者に対して管理者が求めることのできる質問および適切な返答を識別する。個人的情報（７０）は、一般的には所有者以外の何人も知らない過去の個人的な出来事、遠縁の親戚の名前、または偽装を試みた人物が知らないような他のどのような変わった情報をも含む。

【００３６】個人情報フィールドにおいて規定される情報は、また、管理者が疑わしい偽装者からコンピュータを取り戻そうと試みるべきかどうか、所有者が、管理者が要求することを望む証拠品の性質および／または程度、例えば電話での声の要求、デジタル署名、手書きの署名、公証人による認証要求の引き渡し、個人面接などの、疑わしい偽装者をどのように扱うかに関する命令を含んでもよい。このようにして、機密情報が漏洩する前に管理者が用いるべき好ましいプロトコルは、疑わしい不正使用に直面して管理者が為すべきことと共にユーザによって規定される。個人秘密情報が機密情報検索のために実際に使用される場合、そのデータは後に新規の情報に置き換えるべきである。

【００３７】図４は、典型的な預託記録（８０）を示すデータ構造である。預託記録８０は、好ましくは平文で管理者を識別する任意の管理者識別フィールド８２を含む。預託記録は、また、例えば図２に関連して説明した情報を用いて、所有者を識別する任意の「標準」情報フィールド８４を含む。この標準情報は、所望する場合は、好ましい実施例と同様に暗号化してもよい。預託記録８０は、また、図３に関連して示し、上述したような管理者に対するアドバイス、命令および要求を伴う個人識別情報を含むフィールド８６を有する。さらに、預託記録８０は、例えば、ユーザのコンピュータ内に記憶されているデータを解読する全パスワードを含む機密情報フィールド８８を含む。または、機密情報は、機密が複数の管理者間で分割されている場合には「分割」してもよい。「分割」情報の場合、複数の預託構成要素が作成され、それぞれの異なる管理者の各公開鍵のもとで暗号化される。分割預託は、情報が数人の管理者によって検索され、ユーザの機密を再構成可能にするために組み合わされるよう要求することができる。このことを行う周知の方法は、シャミール（ＲＳＡ公開鍵暗号手法の創作者の一人）の技術によって説明される技術を含み、数多くある。この場合、ユーザは、管理者の幾つかの必要な部分集合（様々な許可された部分集合は、機密が預託される際に限定され、例えば３個から２個などになる）に自分のＩＤを確信させなければならない。分割鍵法の利点は、一人の管理者が故意にまたは誤ってシステムを傷

つけることが不可能であることである。

【００３８】預託記録８０は、また、フィールド８２、８４、８６および８８のハッシュをフィールド９０内に含む。さらに、記録８０は、上記情報を暗号化するために用いられるランダム対称（例えばＤＥＳ）鍵の管理者の公開鍵のもとでの暗号化を記憶するためのフィールド９２を含む。複数の管理者および分割鍵預託の場合、各管理者への情報は、個別のランダム対称（ＤＥＳ）鍵のもとで暗号化されるべきであり、そうでなければ、どの管理者もが（鍵分割の保護を破って）他の管理者に属する記録を解読する能力を持つことになるであろう。

【００３９】図５は、本発明の典型的な実施例のユーザ識別、または定義局面に含まれる操作のシーケンスを示すフローチャートである。図５に示す処理手順は、メニュー駆動型オペレータ指示ルーチンによって、ユーザの選択および返答を要求する。図５に示すルーチンは、好ましくは、ユーザがコンピュータを購入して初期化した際、または新しい機密を預託する際に実行される。当該ルーチンが最初に実行された後、変更しにくい情報（例えば、誕生日、出生地など）が他の方法で入手できる場合、それを再び手に入れる必要は必ずしもない。図５に示す操作が遂行されると、機密情報を含む情報は、図４に示す預託記録フォーマット内に配置される。

【００４０】ユーザが機密、例えばパスワードまたは暗号鍵（または金庫室番号の組み合わせ、スイス銀行の口座番号、コカ・コーラ^{R}の製法など）を預託したいと望む時、ユーザは、初めに一人の管理者または受託者、もしくは複数の受託者を選択する（１０１０）。組織によっては、このことが組織内で規定される。分割機密預託においては、一人以上の管理者が存在しており、預託情報を管理者間でどのように分割するかを決定する方法が幾つかなければならない。個別預託記録およびランダム対称鍵が、各管理者に対して生成される。ユーザが管理者または受託者を選択した後、管理者の公開鍵が取得され（１０１５）、できれば公開鍵および鍵分割再組立て規則を含む管理者の識別が、預託記録フィールド８２に格納される。

【００４１】管理者の一つまたは複数の公開鍵を取得した後、機密情報が取得され、図４（１０１７）に示すフィールド８８に格納される。機密は、ユーザによって供給される場合もあり、また、コンピュータによって内部生成される場合もある（例えば、暗号化鍵を定義する場合）。ブロック１０２０から、ルーチンは、オペレータの指示メッセージのシーケンスによって、例えば図２に示す標準識別情報の蓄積を始め、預託記録フィールド８４（図４）にそのような情報を格納する。その後、オペレータの指示メッセージは、ユーザに個人識別情報、および／または管理者に対するアドバイスおよび命令を供給する機会を与え、そのような情報は図４に示すフィールド８６に格納される。例えばデジタル化された写真、声見本など、より量の大きいデジタル情報は、Ｘ．５００辞書または他の保存場所などの他のソースから容易にアクセスされてもよい。そのような情報は、好ましくは、より小さなハッシュを含むとによって集合体情報に組み込まれる。機密情報の検索を申し込む際には、申込者は、管理者が照合できるように、申込者自身のハッシュによって参照できるような必要な追加のデジタル情報を提供すべきである。どのような場合においても、各識別特徴は、図２に示すように、どの特徴が内包の形（全データ、ハッシュ参照による内包など）と同様に定義されているかを示す明瞭な情報でラベルされる。

【００４２】ブロック１０３０に従って、ルーチンは、集合体データのハッシュを計算し、預託記録８０のフィールド９０内の計算されたハッシュを記憶する。計算されたハッシュは、標準識別情報（フィールド８４）、もしあるならば個人識別情報（フィールド８６）、もしあるならば管理者に対するアドバイス／命令（フィールド８６）、およびフィールド８８からの機密情報（例えば、ユーザの暗号パスワード）に基づく。ハッシュは、ＭＤ５または安全ハッシュアルゴリズム（ＳＨＡ）などの、様々な可能で好ましいハッシングアルゴリズムの内のいずれかを用いて計算される。

【００４３】その後、ランダム対称（例えばＤＥＳ）鍵が生成され（１０４０）、少なくとも、預託記録フィールド８８に記憶されている機密情報、フィールド９０内の集合体情報のハッシュ、およびもしあるならばフィールド８６内の個人識別情報を暗号化するために用いられる。好ましい実施例においては、フィールド８６内の管理者に対するアドバイス／命令は、個人情報の一部として含まれており、好ましくは暗号化される。フィールド８４内の標準識別情報は、紛失の際に、発見者が所有者のＩＤを決定できるようにするため、またはライバルに、管理者を騙すためにねつ造する必要のある特徴についての最小限の情報しか与えないようにするために、その有益度に応じて、その全てまたは一部を暗号化することもできるし、もしくは全く暗号化しないこともできる。

【００４４】ステップ１０５０において、ステップ１０４０に従って生成された対称暗号鍵は、管理者の公開鍵を用いて暗号化される。この暗号化された値は、預託記録８０（１０６０）のフィールド９２内に記憶される。複数の管理者が存在する場合は、情報は、各管理者に特有のランダム対称鍵を用いて暗号化するべきである。

【００４５】ブロック１０６０に従った預託記録８０は、様々な受け入れ可能な位置に記憶してもよい。例えば、預託記録は、保護のために即座に管理者に伝達してもよいし、もしくはユーザが、要求があるまで、または要求する際にフロッピーディスクに書き込んで退避してもよい。または、預託記録８０をハードディスクに記録してもよい。預託機密がハードディスクに対するパスワ

ードである場合、預託機密は、そのように暗号化されていないディスクの一部に記録されなければならない。または、預託記録８０は、独立記憶のために管理者以外の第三者に伝達されてもよい。預託記録の印刷版を作成してもよい。便宜のために、管理者、およびいかにして管理者と通信するかを記述した平文情報（８２）を付加することが望ましいかもしれない。このことは、複数の管理者が存在する場合に、情報の特定部分に関連する特定の管理者、および機密を回復するための充分な部分集合をどの管理者の部分集合が含んでいるのかを見分けるのに役立つ。

【００４６】図６は、申込者が預託された機密情報を検索しようと試みる際に遂行される操作のシーケンスを示すフローチャートである。申込者は、機密情報の正当な所有者であるかもしれないし、または貴重な情報を盗もうとたくらむ偽装者であるかもしれない。ブロック２０１０に示すように、申込者は、例えばデジタル化された写真などの情報のハッシュによってのみ参照することのできる預託記録８０に含まれるアイテムに対する完全な情報と共に、管理者の公開鍵のもとで暗号化された預託情報記録８０を管理者に提供する。申込者は、また、預託された情報と一致する信用証明書を含む証拠書類を管理者に提供する。そのような証拠書類は、例えば、機密情報に対する手書きで署名された要求、申込者の特徴を証明する公証人によって実行された宣誓供述書を含んでもよい。機密情報に対する要求は、預託記録内で規定される同一の公開鍵を用いて証明することが可能でなければならない。さらに、申込者の外見は、フィールド８４において預託記録内に含まれる、図２に示す標準識別情報内に記述の特徴に一致しなければならない。ブロック２０１０の好ましい実施例に従うと、申込者が公開鍵を要求し、その公開鍵のもとで情報が返却されることを申込者が望む公開鍵を定義することができるよう考慮されている。このように、管理者および申込者は、機密情報が通信を妨害する敵に漏洩する危険を全く負うことなく、秘密裡に通信することができる。

【００４７】管理者は、その後、図１に示す通信路１２、もしくは例えば郵送で、またはコンピュータ全体を運搬するなどの他の手続によって、ブロック２０１０（２０２０）において抽出された申込者の預託記録を受け取る。管理者は、記録の残りを暗号化するランダム対称鍵にアクセスするために、秘密個人鍵を用いて預託記録のフィールド９２を解読する（２０３０）。管理者が、ブロック２０３５における検査によって決定される際に、当該個人鍵を用いてフィールド９２を解読することができない場合、検索処理は失敗し、適切な失敗メッセージが申込者のもとに返される（２０３６）。

【００４８】ブロック２０３５における解読検査が成功した場合、管理者は、預託記録内の全フィールドが平文で処理できるようにするために、フィールド８６、８８、９０、および暗号化されている範囲に応じてフィールド８４を解読する（２０４０）。解読操作が成功して、信用のおけるデータが検索可能かどうかを確認するために、ブロック２０４５において検査が為される。解読が成功しなかった場合、適切な失敗メッセージがユーザに通信される（２０４６）。

【００４９】管理者は、その後、預託記録フィールド８４、８６および８８のハッシュを再計算する（２０５０）。再計算されたハッシュが、図４のフィールド９０内の供給されたハッシュ値と一致するかどうかを決定するために、ブロック２０６０において検査が為される。当該ハッシュ値が一致しない場合、申込者の預託データは、信頼性のないものであり、改ざんされた暗号テキストを反映している可能性があるため、検索が許可されない。従って、信用して検索処理を遂行することはできず、適切なメッセージが申込者に通信される（２０６１）。

【００５０】ハッシュが一致した場合、預託記録が正しい形で引き渡されたことが管理者に保証される。管理者は、その後、預託記録データを吟味し（２０７０）、預託された識別が、ブロック２０１０において管理者に供給された申込者の証拠の信用証明書によって確証されるかどうかを決定する。それにより、管理者は、公証人からの宣誓供述書、声通信などによって供給されたデータが、預託記録データと一致するかどうかを決定する。受け取った信用証明書に基づいて、申込者が正当な所有者のようであるか、または（従業員によって管理されている機密の会社の所有者であるなどの理由から）データに対して正真正銘の権利を有しているのかが、ブロック２０８０において決定される。

【００５１】ブロック２０８０における検査の結果、申込者が当該機密情報に対して権利を有することが示された場合、管理者は、申込者の要求によって定義された公開鍵（２０１０）、または預託された情報内で定義されている公開鍵（図２の３０）を用いて、図４のフィールド８８に含まれる預託された秘密値を暗号化し、暗号化された機密情報を申込者に受け渡す（２１４０）。

【００５２】ブロック２０８０での検査の結果、申込者が機密情報に対して権利を有していることが確認されない場合、申込者が偽装者であるかどうかを決定するための検査がブロック２０９０において為される。ブロック２０９０における検査により、申込者が偽装者であると決定するのに充分な情報があることが判明した場合、ルーチンは分岐してブロック２１３０に進み、そこで管理者は、真の所有者または警察に知らせたり、偽装者についての更なる情報を得ようと試みたり、および／または盗まれたコンピュータ機器を取り返そうと試みるなどの適切な行動を取る。管理者が取る行動は、好ましくは、管理者に対するアドバイス／命令および要求の一部としてフィールド８６内の預託記録において規定される。

【００５３】ブロック２０９０における検査の結果、申込者が偽装者であるのか、またはそうでないのかを確認するための充分な情報がないと示された場合、ルーチンは分岐して２１００に進み、識別の不明瞭さを解決するために必要な追加の信用証明書を申込者に要求する。そのような追加の情報は、預託記録内のハッシュが参照してきており、最初の申し込み、預託情報内に供給されている個人識別情報によって提示される質問、個人面接、電話での会話、公証人によって認証された署名、預託された情報において規定される公開鍵に基づく要請／返答、および運転免許書などの独立した第三者によって認証された証書には含まれないデジタルバイオメトリクス（例えば、デジタル化された写真）のソースに対する要求を含んでもよい。問題となっている実際のコンピュータの提示は、特に、個人識別情報フィールド８６におけるアドバイスによって規定されている場合、要求してもよい。申込者のＩＤを確認するために必要な他の情報と共に、より信頼性のある、またはより認証されている信用証明書を要求してもよい。信用証明書を電子的に要求する場合、その要求は、申込者の信用証明書と共に供給される公開鍵、または預託情報内に含まれる公開鍵のいずれかによって暗号化してもよい。

【００５４】申込者がブロックにおいて追加の質問を受信し（２１１０）、それが暗号化されている場合、申込者は適切な個人鍵を用いてそれを解読する。申込者は、追加の信用証明書を提供することによってその要求に従うか、または管理者に自らの本当のＩＤを納得させるために必要ないかなる手段をも講じる。このことは、外見、電話での通話、または預託された個人識別情報内で問われる質問に返答することを含んでもよい。電子的に返答を行う場合、それらは、管理者の公開鍵のもとで暗号化することができる。

【００５５】ブロック２１２０に示すように、管理者は、追加の情報を受け取り、必要に応じてそれを解読する。追加の信用証明書は既に手中にあるものと結合され、ルーチンは分岐して、評価処理を再開するためにブロック２０７０へ戻る。評価処理は、ブロック２０８０において申込者が本物であるかを確認するため、またはブロック２０９０において偽装者であるかを確認するために必要な回数だけ繰り返される。

【００５６】申込者が本物である場合、ブロック２１４０において示すように、機密情報は、預託記録（３０）を伴う個人鍵のもとで暗号化されて、または２０１０における（現在確認される）申し込みによって供給される際に、申込者のもとに送信される。申込者は、供給された預託機密情報を受取り、適切な個人鍵を用いて供給された機密情報を解読する（２１５０）。

【００５７】機密分割鍵が用いられ、それにより、各分割鍵管理者がユーザの機密の構成要素を受け取る場合、処理は全機密が蓄積されるまで続けられる。受け取られた預託情報が、預託された機密の最後の部分（またはほんの一部）であるかどうかを決定するために、ブロック２１６０において検査が為される。例えば、機密情報の二分の一または三分の一をそれぞれ預託するために、二人または三人の管理者が存在してもよい。ブロック２１５０－２１７０において示す折り返しは、各管理者から全機密情報を集めるための処理を示している。いったん全機密情報が受け取られ、ブロック２１６０において決定されると、申込者は、機密情報、例えば自分のパスワードを回復するために充分な情報を取り戻す。

【００５８】２１６０における検査の結果、一人またはそれ以上の受託者から、より多くの機密情報の部分要素を受け取る必要のあることが示された場合、ルーチンは分岐して２１７０に進み、そこで処理手続は、本来の機密情報を集めることのできるのに充分な部分要素が検索されるまで、分割機密の追加として預託された部分を確実に取得できるようにするために遂行される。ブロック２１７０における処理が、受託者の内の一人が追加の情報を要求していることを示す場合、処理は分岐してブロック２１１０に進み、そこで申込者に対する追加の識別質問を処理する。２１７０における処理の結果、管理者が機密情報の失われた部分を供給することになった場合、当該情報はブロック２１５０において申込者に提供される。最後に、申込者が機密情報を受け取る資格がある場合、全機密情報が集められる。

【００５９】本発明は、現在、最も実用的かつ好ましい実施態様であると考えられるものに関して記述してきたが、本発明は、開示された実施例に限定されるものではなく、それどころか、様々な変更、ならびに特許請求の範囲の意図および有効範囲内に含まれる同等の組み合わせを包含するよう意図されていることを理解していただきたい。

【図面の簡単な説明】

【図１】本発明を使用し得る典型的な通信システムを示すブロック図である。

【図２】ユーザから収集した典型的な「標準」識別預託情報を示す図である。

【図３】後にユーザが、他の命令または情報、もしくは管理者に対するアドバイスと共に質問を受ける個人的な知識を示す典型的な「個人」識別情報データを示す図である。

【図４】典型的な預託記録を示すデータ構造図である。

【図５】ユーザの識別局面または定義局面に含まれる操作のシーケンスを、本発明の典型的な実施例に従って表したフローチャートである。

【図６】申込者が預託された機密情報を検索しようとする時に遂行される操作の典型的なシーケンスを表したフローチャートである。

【符号の説明】

Ａ～Ｎ…端末装置

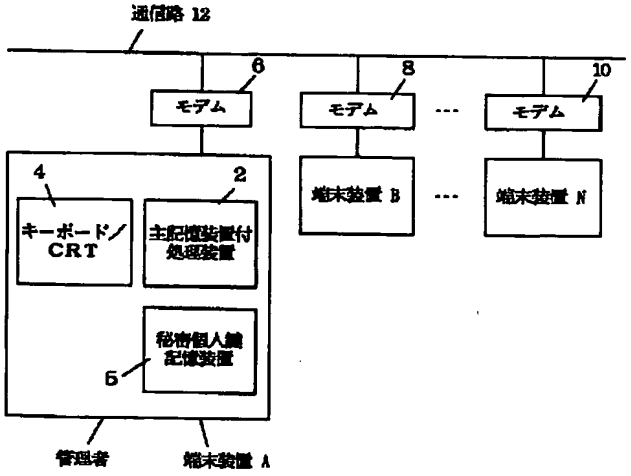
19

2…演算処理装置
4…キーボード／ＣＲＴディスプレイ

20

5…秘密個人鍵記憶装置
6～8…モデム

【図１】



【図２】

標準識別情報 18

	特　徴	タイプ	値
20	氏　名	テキスト	スマイリー・ロバート
22	住　所	テキスト	アメリカ合衆国オハイオ州　45403 ディトン　スノー　イーグルドライブ 651
24	誕生日	テキスト	1956年12月15日
26	出生地	テキスト	ウィルミントン生まれ
28	電話番号	テキスト	513-278-6734
30	ユーザの公開鍵	バイナリ	(バイナリ公開鍵 ALA X.500)
32	会社名	テキスト	フラグストン・ツール・アンド ダイ
34	役　職	テキスト	広報部長
36	上　司	テキスト	ホワイトホール・エミリー・ジェイン
38	社員番号	な　し	(省　略)
40	社会保険番号	テキスト	762-553-8936
42	運転免許証番号	テキスト	オハイオ PC782352
44	身　長	テキスト	5フィート9インチ
46	体　重	テキスト	175ポンド
48	目の色	テキスト	茶　色
50	写　真	ハッシュ	(デジタル化されたイメージのハッシュ)
52	指紋イメージ	な　し	
54	網膜パラメータ	な　し	
56	声紋メッセージ	な　し	
58	筆跡イメージ	PCX	筆跡のイメージ
60	筆法情報	な　し	
62	DNAパターン	な　し	
64	その他		

【図３】

個人識別情報　70

以下の２つの質問によって私を識別してください：

Q：私が３歳だった頃、私の姉は私を何と呼んでいましたか？
A：「ポピー鳥」

Q：私が最初に飼ったペットは何でしたか？
A：「ヘンリー」という名の亀

追加のアドバイスおよび要求：

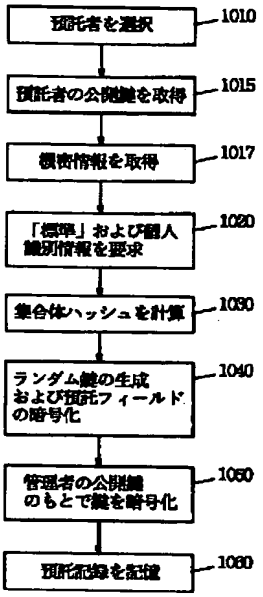
私は、偽装が疑われた場合に、管理者が私のコンピュータを物理的に改善しようと試みることをここに許可します。同時に、未許可のアクセスを試みるいかなる人物に関しても、できる限り多くの情報を入手するよう要求します。先に提供した連絡情報を用いて、私に通知していただけるようお願いします。

【図４】

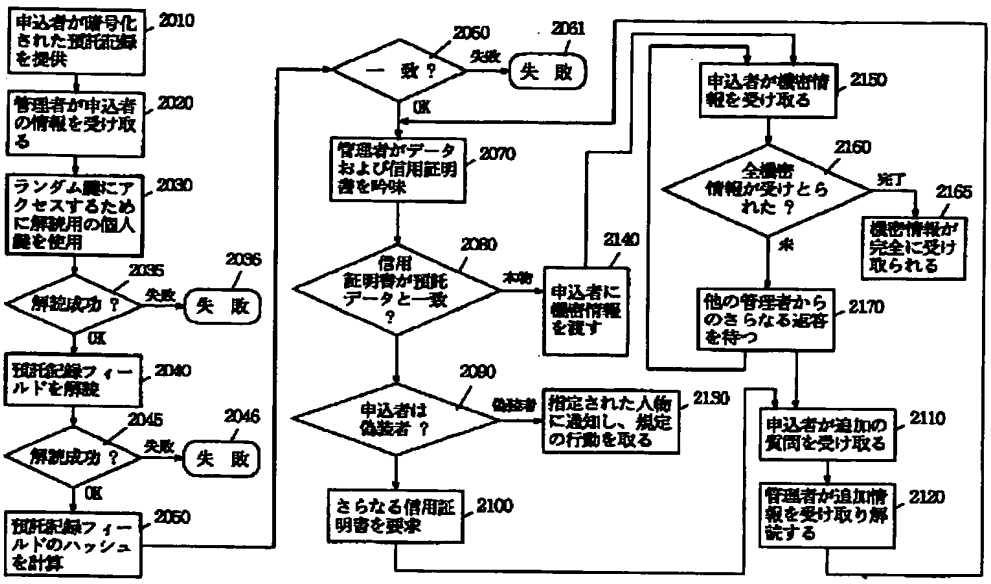
預託記録　80

82	１： 管理者を識別する任意の情報
	以下は、任意に暗号化されている：
84	２： 所有者を識別する「標準」情報
	以下は暗号化されている：
86	３： ａ．個人識別情報；ならびに ｂ．アドバイス、管理者に対する命令および要求
88	４：機密情報 （例えば、ユーザのコンピュータ内に記憶されているデータを解読するパスワード） または、機密が複数の管理者間で分割されている場合、機密の「一部」
90	５：上記情報のハッシュ
92	６：上記情報を暗号化するために用いられるランダム対称（ＤＥＳ）鍵の管理者の公開鍵のもとでの暗号化

【図５】



【図６】



フロントページの続き

(51)Int.Cl.⁶	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ　9/32				